

What is claimed is:

1 1. A method for detecting least significant bit ("LSB") embedding of a
2 message hidden in randomly scattered samples of an alleged cover image, comprising
3 the steps of:

4 dividing the alleged cover image into a plurality of disjoint groups of adjacent
5 samples;

6 defining a discrimination function that assigns a real number to each member
7 of said plurality, thereby capturing the smoothness of each of said groups;

8 defining on said plurality at least one invertible operation that comprises a
9 permutation of sample values, whereby values of said samples are invertibly
10 perturbed by a small amount;

11 applying said discrimination function and said ~~flipping operation~~ ^{invertible operation} to define in
12 said plurality three types of sample groups, (R)egular, (S)ingular, and (U)nusable,
13 each of said types being defined for both positive and negative operations;

14 plotting both positive and negative R and S for said alleged cover image on an
15 RS diagram;

16 constructing four curves of said RS diagram and calculating their intersections
17 by extrapolation; and

18 determining the existence or nonexistence of a secret message from said
19 intersections.

1 2. The method of claim 1, further including the step, if said secret message is
2 determined to exist, of estimating a length thereof.

1 3. The method of claim 2, wherein each of said samples is a pixel value.

1 4. The method of claim 3, wherein said pixel value is a grayscale.

1 5. The method of claim 3, wherein said pixel value is a color.

1 6. The method of claim 2, wherein each of said samples is an index to a palette
2 of color values.

1 7. The method of claim 1, wherein said step of constructing further comprises
2 arithmetically averaging the x coordinates of said intersections, thereby detecting said
3 hidden message, if it exists, and estimating a length thereof.

1 8. The method of claim 2, wherein said step of estimating further comprises
2 determining a length p of said hidden message, if it exists, by rescaling the x -axis of
3 said RS diagram so that $p/2$ becomes 0 and $100 - p/2$ becomes 1, whereby an x -
4 coordinate of an intersection is a root of the following quadratic equation:

5
$$2(d_1 + d_0)x^2 + (d_{-0} - d_{-1} - d_1 - 3d_0)x + d_0 - d_{-0} = 0,$$

6 where $d_0 = R_M(p/2) - S_M(p/2)$, $d_1 = R_M(1 - p/2) - S_M(1 - p/2)$, $d_{-0} = R_{-M}(p/2) - S_{-M}(p/2)$,
7 $d_{-1} = R_{-M}(1 - p/2) - S_{-M}(1 - p/2)$, and said message length p is calculated from the root
8 x whose absolute value is smaller,

9
$$p = x/(x-1/2).$$

1 9. Apparatus for detecting least significant bit ("LSB") embedding of a
2 message hidden in randomly scattered samples of an alleged cover image, which
3 comprises:

4 means for dividing said alleged cover image into a plurality of disjoint groups
5 of adjacent samples;

6 first means for defining effective for defining a discrimination function that
7 assigns a real number to each member of said plurality, thereby capturing the
8 smoothness of each of said groups;

9 second means for defining effective for defining on said plurality at least one
10 invertible operation that comprises a permutation of sample values, whereby values of
11 said samples are invertibly perturbed by a small amount;

12 means for applying said discrimination function and said ~~flipping operation~~
13 define in said plurality three types of sample groups, (R)egular, (S)ingular, and
14 (U)nusable, each of said types being defined for both positive and negative
15 operations;

16 means for plotting both positive and negative R and S for said alleged cover
17 image on an RS diagram;

18 means for constructing four curves of said RS diagram;

19 means for calculating the intersections of said four curves by extrapolation;

20 and

21 first means for determining effective for determining from said intersections
22 the existence or nonexistence of a secret message.

1 10. The apparatus of claim 9, further including means for estimating a length
2 of said secret message if said secret message is determined to exist.

1 11. The apparatus of claim 10, wherein each of said samples is a pixel value.

1 12. The apparatus of claim 11, wherein said pixel value is a grayscale.

1 13. The apparatus of claim 11, wherein said pixel value is a color.

1 14. The apparatus of claim 10, wherein each of said samples is an index to a
2 palette of color values.

1 15. The apparatus of claim 9, wherein said means for constructing and
2 calculating is further effective for arithmetically averaging the x coordinates of said
3 intersections, thereby detecting said hidden message and estimating a length thereof.

1 16. The apparatus of claim 10, wherein said means for estimating is effective
2 for determining a length p of said hidden message by rescaling the x -axis of said RS
3 diagram so that $p/2$ becomes 0 and $100 - p/2$ becomes 1, whereby an x -coordinate of
4 an intersection is a root of the following quadratic equation:

5
$$2(d_1 + d_0)x^2 + (d_{-0} - d_{-1} - d_1 - 3d_0)x + d_0 - d_{-0} = 0,$$

6 where $d_0 = R_M(p/2) - S_M(p/2)$, $d_1 = R_M(1 - p/2) - S_M(1 - p/2)$, $d_{-0} = R_{-M}(p/2) - S_{-M}(p/2)$,
7 $d_{-1} = R_{-M}(1 - p/2) - S_{-M}(1 - p/2)$, and said message length p is calculated from the root
8 x whose absolute value is smaller,

9
$$p = x/(x-1/2).$$

1 17. A computer-readable storage medium embodying program instructions for
2 a method for detecting least significant bit ("LSB") embedding of a message hidden
3 in randomly scattered samples of an alleged cover image, said method comprising the
4 steps of:

5 dividing said alleged cover image into a plurality of disjoint groups of
6 adjacent samples;

7 defining a discrimination function that assigns a real number to each member
8 of said plurality, thereby capturing the smoothness of each of said groups;

9 defining on said plurality at least one invertible operation that comprises a
10 permutation of sample values, whereby values of said samples are invertibly
11 perturbed by a small amount;

12 applying said discrimination function and said ~~flipping operation~~ *invertible operation* to define in
13 said plurality three types of sample groups, (R)egular, (S)ingular, and (U)nusable,
14 each of said types being defined for both positive and negative operations;

15 plotting both positive and negative R and S for said alleged cover image on an
16 RS diagram;

17 constructing four curves of said RS diagram and calculating their intersections
18 by extrapolation; and

19 determining the existence or nonexistence of a secret message from said
20 intersections.

1 18. The computer-readable storage medium of claim 17, said method further
2 including the step, if said secret message is determined to exist, of estimating a length
3 thereof.

1 19. The computer-readable storage medium of claim 17, said method further
2 including, in said step of constructing, arithmetically averaging the x coordinates of
3 said intersections, thereby detecting said hidden message, if it exists, and estimating a
4 length thereof.

1 20. The computer-readable storage medium of claim 17, said method further
2 including, in said step of estimating, determining a length p of said hidden message, if
3 it exists, by rescaling the x -axis of said RS diagram so that $p/2$ becomes 0 and $100 -$
4 $p/2$ becomes 1, whereby an x -coordinate of an intersection is a root of the following
5 quadratic equation:

6
$$2(d_1 + d_0)x^2 + (d_{-0} - d_{-1} - d_1 - 3d_0)x + d_0 - d_{-0} = 0,$$

7 where $d_0 = R_M(p/2) - S_M(p/2)$, $d_1 = R_M(1 - p/2) - S_M(1 - p/2)$, $d_{-0} = R_{-M}(p/2) - S_{-M}(p/2)$,
8 $d_{-1} = R_{-M}(1 - p/2) - S_{-M}(1 - p/2)$, and said message length p is calculated from the root
9 x whose absolute value is smaller,

10
$$p = x/(x-1/2).$$